

LAW OFFICES
SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC

2100 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20037-3213
TELEPHONE (202) 293-7060
FACSIMILE (202) 293-7860
www.sughrue.com

November 27, 2000

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Re: Application of Jae-han PARK
AUTHENTICATION METHOD FOR ESTABLISHING CONNECTION
BETWEEN DEVICES
Our Ref. Q61823

Dear Sir:

Attached hereto is the application identified above including thirty-two (32) sheets of the specification, claims, and seven (7) sheets of drawings. **The requisite U.S. Government Filing Fee, executed Declaration and Power of Attorney and Assignment will be submitted at a later date.**

The Government filing fee is calculated as follows:

Total claims	14 - 20	=		x	\$18.00	=	\$0.00
Independent claims	3 - 3	=		x	\$80.00	=	\$0.00
Base Fee							\$710.00
TOTAL FEE							\$710.00

Priority is claimed from November 25, 1999 based on KR Application No. 99-52658.
The priority document is enclosed herewith.

Since the anniversary of the priority date fell on a Saturday, the filing of this application on Monday, November 27, 2000, is sufficient to obtain the benefit of priority.

Respectfully submitted,
SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
Attorneys for Applicant

By: Darryl Mexic
Darryl Mexic
Registration No. 23,063

DM/plr

CERTIFIED COPY OF
PRIORITY DOCUMENT

대한민국 특허청
KOREAN INDUSTRIAL
PROPERTY OFFICE



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Industrial
Property Office.

출원번호 : 1999년 특허출원 제52658호
Application Number

출원년월일 : 1999년 11월 25일
Date of Application

출원인 : 삼성전자 주식회사
Applicant(s)



1999년 12월 9일

특허청

COMMISSIONER



【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0007
【제출일자】	1999.11.25
【국제특허분류】	H04L
【발명의 명칭】	블루투스 링크 관리자간의 인증방법
【발명의 영문명칭】	Authentication method between link managers of bluetooth
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	1999-009556-9
【대리인】	
【성명】	권석흠
【대리인코드】	9-1998-000117-4
【포괄위임등록번호】	1999-009576-5
【대리인】	
【성명】	이상용
【대리인코드】	9-1998-000451-0
【포괄위임등록번호】	1999-009577-2
【발명자】	
【성명의 국문표기】	박재한
【성명의 영문표기】	PARK, Jae Han
【주민등록번호】	740208-1683110
【우편번호】	449-900
【주소】	경기도 용인시 기흥읍 서천리 163-7 리빙타운 305호
【국적】	KR

【취지】

특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대
리인 이영

필 (인) 대리인

권석홍 (인) 대리인

이상용 (인)

【수수료】

【기본출원료】 18 면 29,000 원

【가산출원료】 0 면 0 원

【우선권주장료】 0 건 0 원

【심사청구료】 0 항 0 원

【합계】 29,000 원

【첨부서류】

1. 요약서·명세서(도면)_1통

【요약서】**【요약】**

본 발명은 블루투스 통신환경에서 운영되는 장치간에 링크를 설정할 때, 상대측 링크 관리자의 인증조건에 따라 링크관리자간에 인증절차를 수행하는 방법을 개시한다. 본 발명에 따른 방법은, 인증요구 개시측 링크 관리자로부터 인증요구 수신측 링크 관리자로 인증요구 메시지를 송출하고; 인증요구 메시지에 대한 인증 응답 메시지가 수신되면, 인증요구 개시측 링크 관리자는 현재의 링크설정단계에 따른 소정의 메시지를 인증요구 수신측 링크 관리자로 송출하면서 저장하고; 소정의 메시지가 수신되면, 인증요구 수신측 링크 관리자는 자신의 인증조건을 체크하고; 인증조건을 체크한 결과, 상호인증이 필요하지 않은 경우에는 소정의 메시지에 대한 응답 메시지를 인증요구 개시측 링크 관리자로 송출하고; 인증조건을 체크한 결과, 상호인증이 필요한 경우에는 소정의 메시지를 저장하고, 인증요구 개시측 링크 관리자로 인증요구 메시지를 송출하고; 인증요구 개시측 링크 관리자로부터 인증요구 메시지에 대한 응답 메시지가 수신되면, 저장된 소정의 메시지에 대한 응답 메시지를 인증요구 개시측 링크 관리자로 송출하고; 인증요구 수신측 링크 관리자로부터 소정의 메시지에 대한 응답 메시지가 수신되면, 인증절차를 완료하는 단계들을 포함한다. 따라서, 블루투스 통신환경에서 운영되는 장치간에 정확한 링크설정 결과를 얻을 수 있다.

【대표도】

도 2

【명세서】**【발명의 명칭】**

블루투스 링크 관리자간의 인증방법 {Authentication method between link managers of bluetooth}

【도면의 간단한 설명】

도 1은 본 발명에 따른 방법을 수행하기 위한 장치의 기능 블록도이다.

도 2는 본 발명에 따른 링크 관리자간의 인증방법을 수행하는데 있어서 인증 개시측의 동작 흐름도이다.

도 3은 본 발명에 따른 링크 관리자간의 인증방법을 수행하는데 있어서 인증요구 수신측의 동작 흐름도이다.

【발명의 상세한 설명】**【발명의 목적】****【발명이 속하는 기술분야 및 그 분야의 종래기술】**

<4> 본 발명은 블루투스(Bluetooth)에 관한 것으로, 특히, 블루투스 통신환경에서 운영되는 장치간에 링크(link)를 설정하기 위한 링크 관리자(link manager)간의 인증(authentication) 방법에 관한 것이다.

<5> 블루투스는 각종 전자기기간에 물리적인 케이블없이 무선주파수(RF)를 이용하여 고속으로 데이터를 송수신하기 위해 제안된 근접 무선 데이터 통신 규격으로서, 음성 부호화방식의 CVSD(Continuous Variable Slope Delta Modulation)를 채용하여 공간의 제한 없이 사방에서 문자 데이터는 물론이고 음성 전송도 가능하게 하는 장점을 갖고 있다.

<6> 이러한 블루투스 통신환경에서 운영되는 장치간에 통신을 하기 위해서는 연결 (connection)과정이 선행되어야 하는데, 이 연결과정은 크게 RF동기를 맞추는 과정, 통신하고자 하는 장치에 구비되어 있는 링크 관리자간의 링크 설정과정 및 채널설정과정으로 분류될 수 있다. 그러나, 아직까지 블루투스 통신환경에 대한 규격 제정이 완벽하게 이루어지지 않았기 때문에 상술한 연결과정을 비롯한 여러 부분에서 해당되는 규정 제정을 위한 연구가 다각도로 진행되고 있다.

【발명이 이루고자 하는 기술적 과제】

<7> 본 발명은 상술한 추세에 따라 안출된 것으로, 블루투스 통신환경에서 운영되는 장치간에 링크를 설정하기 위해 각 장치에 구비되어 있는 링크 관리자간에 수행되는 인증방법을 제공하는데 그 목적이 있다.

<8> 본 발명의 다른 목적은 블루투스 통신환경에서 운영되는 장치간에 링크를 설정할 때, 상대 장치의 인증조건에 따라 인증절차를 수행하는 링크 관리자간의 인증방법을 제공하는데 있다.

【발명의 구성 및 작용】

<9> 본 발명이 이루고자 하는 목적을 달성하기 위하여 본 발명에 따른 방법은, 블루투스 통신환경에서 운영되는 장치에 구비되어 있는 링크 관리자간에 링크를 설정하는 방법에 있어서, 인증요구 개시측 링크 관리자로부터 인증요구 수신측 링크 관리자로 인증요구 메시지를 송출하는 제 1 단계; 인증요구 메시지에 대한 인증 응답 메시지가 수신되면, 인증요구 개시측 링크 관리자는 현재의 링크설정단계에 따

른 소정의 메시지를 인증요구 수신측 링크 관리자로 송출하면서 저장하는 제 2 단계;소정의 메시지가 수신되면, 인증요구 수신측 링크 관리자는 자신의 인증조건을 체크하는 제 3 단계; 인증조건을 체크한 결과, 상호인증이 필요하지 않은 경우에는 소정의 메시지에 대한 응답 메시지를 인증요구 개시측 링크 관리자로 송출하는 제 4 단계; 인증조건을 체크한 결과, 상호인증이 필요한 경우에는 소정의 메시지를 저장하고, 인증요구 개시측 링크 관리자로 인증요구 메시지를 송출하는 제 5 단계; 인증요구 개시측 링크 관리자로부터 인증요구 메시지에 대한 응답 메시지가 수신되면, 저장된 소정의 메시지에 대한 응답 메시지를 인증요구 개시측 링크 관리자로 송출하는 제 6 단계; 인증요구 수신측 링크 관리자로부터 소정의 메시지에 대한 응답 메시지가 수신되면, 인증절차를 완료하는 제 7 단계를 포함하는 것이 바람직하다.

<10> 이하, 첨부된 도면을 참조하여 본 발명을 상세히 설명한다.

<11> 도 1은 본 발명에 따른 링크 관리자간의 인증방법을 수행하기 위한 장치의 기능 블럭도로서, 블루투스방식으로 통신하기를 원하는 장치에 대하여 인증요구 개시측(100)과 인증요구 수신측(110)으로 구분한 것이다. 인증요구 개시측(100)과 인증요구 수신측(110)은 각각 호스트 제어 인터페이스부(Host Controller Interface)(102)(112), 링크 관리자(Link Manager)(106)(116), 종단부(108)(118)를 포함한다.

<12> 호스트 제어 인터페이스부(102)(112)는 각각 대응되는 호스트(미 도시됨)와 데이터 송수신을 하기 위하여 레이어 2에 해당되는 정합처리를 수행할 수 있도록

구현된 것으로, 인증요구 개시측(100)과 인증요구 수신측(110)이 해당되는 호스트(미 도시됨)와 분리된 모듈구조로 구성된 경우이다. 호스트(미 도시됨)는 광의적으로는 블루투스 기능을 채용한 장치이고, 협의적으로는 블루투스 기능을 채용한 장치내에 구비되어 해당 장치의 중앙제어부(미 도시됨)와 연동되도록 구성된 블루투스 호스트이다. 이 블루투스 호스트는 채널을 설정하기 위해 레이어 2에 해당되는 기능을 수행하는 L2 CAP(Logical Link Control and Adaptation Protocol) 및 응용(Application)기능 등을 수행할 수 있도록 구현된다.

<13> 링크 관리자(106)(116)는 블루투스 통신환경에서 통신하고자 하는 장치간에 링크 설정 및 해제, 설정된 링크를 운영하는 기능 등을 수행하도록 구현된다. 종단부(108),(118)는 블루투스 통신환경에서 통신하고자 하는 장치간에 고주파(RF) 통신이 가능하도록 고주파 동기를 일치시키고, 비트를 심볼(symbol)로 변환시키는 등의 고주파 처리와 베이스 밴드(Baseband) 제어로 구분될 수 있다. 베이스 밴드 제어 기능으로는 부호화/암호화(coding/ciphering), 패킷 핸들링, 주파수 호핑(hopping) 등이 존재한다.

<14> 이와 같은 호스트 제어 인터페이스부(102)(112), 링크 관리자(106)(116), 종단부(108)(118)로 구성된 인증요구 개시측(100) 및 인증요구 수신측(110)은 상술한 바와 같이 호스트와 분리된 구조인 경우에 블루투스 모듈이라고 칭하기도 한다.

<15> 이러한 블루투스 모듈들은 해당되는 호스트의 요구에 의해 통신을 원하는 장치와 고주파 동기를 일치시킨 후, 링크를 설정하게 된다. 이 링크 설정은 각 장치측에 해당되는 링크 관리자(106)(116)간에 링크 인증절차를 거쳐 수행된다. 본 발명에 따른 링크 관리자간의 인증절차는 도 2 및 도 3에 도시된 바와 같이 이루어진다. 도 2는 본 발명에 따른 링크 관리자간의 인증방법을 수행하는데 있어서 인증 개시측의 동작 흐름도이고, 도 3은 본 발명에 따른

링크 관리자간의 인증방법을 수행하는데 있어서 인증요구 수신측의 동작 흐름도이다.

- <16> 그러면, 도 1를 참조하여 도 2 및 도 3에 도시된 본 발명에 따른 링크 관리자간의 인증 방법에 대해 설명하면 다음과 같다.
- <17> 먼저, 인증요구 개시측(100)의 링크 관리자(106)가 종단부(108)를 경유하여 인증요구(Authentication Request) 메시지(LMP_au_rand)를 송출하면, 단계 302에서 인증요구 수신측(110)의 링크 관리자(116)는 종단부(118)를 통해 인증요구 메시지를 수신하고, 단계 304로 진행되어 수신된 인증요구 메시지에 대응되는 인증응답 메시지(LMP_sres)를 종단부(118)를 경유하여 인증요구 개시측(100)으로 송출한다. 이에 따라 인증요구 개시측(100)의 링크 관리자(106)는 단계 204에서 종단부(108)를 경유하여 인가되는 인증요구 메시지에 대응되는 응답 메시지를 수신한다.
- <18> 응답 메시지를 수신한 링크 관리자(106)는 단계 206으로 진행되어 수신된 응답 메시지가 유효한(valid) 지를 판단한다. 판단방법은 단계 202에서 송출된 인증요구 메시지에 포함되어 있는 랜덤(random) 정보와 자신이 보유하고 있는 키(Key)정보를 이용하여 이루어진다. 즉, 키 정보는 양측의 링크 관리자(106)(116)가 동일한 정보를 갖고 인증요구 수신측의 링크 관리자(116)가 인증요구 응답 메시지를 송출할 때 인증요구 메시지에 포함된 랜덤 정보와 자신이 보유하고 있는 키정보를 이용하여 계산한 응답정보를 포함시켜 송출한다. 인증요구 개시측 링크 관리자(106)는 인증요구 응답 메시지에 포함된 상술한 응답정보와 자신이 보유하고 있는 키정보와 송출한 랜덤정보를 이용한 연산결과를 비교하여 현재 수신된 인증요구 응답 메시지가 유효한 지를 판단하도록 구현할 수도 있다.
- <19> 단계 206의 판단결과, 수신된 인증응답 메시지가 유효하지 않으면, 링크 관리자(106)는 해당되는 인증 작업이 실패(fail)한 것으로 판단하고, 단계 208에서 인증 실패에 따른 작

업을 수행한다. 즉, 해당되는 호스트(미 도시됨)측과 인증요구 수신측(110)으로 해당되는 인증작업이 실패되었음을 통보한다. 그리고, 단계 210으로 진행되어 해당되는 인증 작업을 종료한다.

<20> 그러나, 단계 206에서 판단한 결과, 수신된 인증응답 메시지가 유효한 것으로 판단되면, 링크 관리자(106)는 단계 212로 진행되어 현재 링크설정단계가 링크 설정을 위한 초기 접속단계(pairing)에 해당되는 지를 체크한다. 이는 링크 관리자(106)에 구비되어 있는 관리 테이블(미 도시됨)에 저장된 데이터가 존재하는 지에 따라 결정되는 것으로, 상술한 관리 테이블(미 도시됨)에 저장된 데이터가 존재하지 않으면, 링크설정을 위한 초기 접속단계로 판단한다. 이와 같이 현재 링크설정단계가 초기 접속단계에 해당되는 경우에, 단계 206에서 이용한 키는 초기 키(initialize key)정보이므로, 양자간에 이용할 링크 키(link key)를 생성하여야 한다. 링크 키는 설정할 링크에 할당될 식별정보이다.

<21> 따라서, 단계 212에서 체크한 결과, 현재 링크설정단계가 링크설정을 위한 초기 접속단계에 해당되면, 링크 관리자(106)는 단계 214로 진행되어 링크 키를 생성하기 위한 메시지를 종단부(108)를 경유하여 인증요구 수신측(110)으로 송출하고, 송출한 메시지를 미 도시된 관리 테이블에 저장한다. 이 때, 송출되는 메시지는, 링크 관리자(106)가 보유하고 있는 키 정보와 링크 관리자(116)가 보유하고 있는 키 정보를 조합한 결과를 이용하여 링크 키 정보를 생성하고자 할 때에는 조합키 메시지(LMP_comb_key)가 되고, 링크 관리자(106)에 보유하고 있는 키정보만을 이용하여 링크 키 정보를 생성하고자 할 때에는 단일 키 메시지(LMP_unit_key)가 된다.

<22> 단계 214에서 링크 키 생성을 위한 메시지가 송출되면, 인증요구 수신측의 링크 관리자(116)는 단계 306에서 단계 308로 진행되어 자신의 인증조건을 체크한다. 자신의 인증

조건은 상호 인증(Mutual authentication)절차가 고려되어야 하는 지를 판단할 수 있는 정보로서, 인증 인에이블(Authentication_enable) 정보를 이용할 수 있다. 예를 들어, 인증 인에이블정보가 '0x00'로 설정되어 있으면, 상호인증이 고려될 필요가 없는 것으로 판단되고, '0x01'로 설정되어 있으면, 상호인증이 고려될 필요가 있는 것으로 판단된다.

<23> 단계 308의 판단결과, 상호인증이 고려될 필요가 없으면, 단계 310으로 진행되어 링크 키 생성을 위한 메시지를 중단부(118)를 경유하여 인증요구 개시측(100)으로 송출한다. 이 때, 송출되는 메시지는 단계 214에서 송출된 메시지와 관계없이 링크 관리자(106)가 보유하고 있는 키정보와 링크 관리자(116)가 보유하고 있는 키정보를 조합한 결과를 이용하여 링크 키 정보를 생성하고자 할 때에는 조합 키 메시지(LMP_comb_key)가 되고, 링크 관리자(116)가 보유하고 있는 키 정보만을 이용하여 링크 키 정보를 생성하고자 할 때에는 단일 키 메시지(LMP_comb_key)가 된다.

<24> 그 다음 링크 관리자(116)는 단계 312로 진행되어 해당되는 인증절차를 완료하고, 생성된 링크 키를 기반으로 한 링크를 설정한 후, 단계 314로 진행되어 링크설정작업을 완료한다.

<25> 그러나, 단계 308의 판단결과, 상호인증이 고려될 필요가 있으면, 링크 관리자(116)는 단계 308에서 단계 316으로 진행되어 수신한 링크 키 생성을 위한 메시지를 미 도시된 관리 테이블에 저장한 뒤, 단계 318로 진행되어 인증요구 메시지를 중단부(118)를 경유하여 인증요구 개시측(100)으로 송출한다.

<26> 한편, 인증요구 개시측(100)의 링크 관리자(106)는 단계 214에서 링크 생성을 위한 메시지를 송출한 후, 단계 216에서 상대장치인 인증요구 수신측(110)으로부터 메시지가 수신되면, 단계 218로 진행되어 수신된 메시지가 링크 키 생성을 위한 메시지

(LMP_comb_key 또는 LMP_unit_key)인지 인증요구 메시지(LMP_auth_rand)인지를 분석한다. 분석은 수신된 메시지의 페이로드(payload)에 실려 있는 식별정보(op code)에 대한 해석으로 이루어진다.

<27> 분석결과, 링크 키 생성을 위한 메시지이면, 단계 220으로 진행되어 해당되는 링크 키를 생성한다. 이 때, 링크 관리자(106)는 링크 관리자(116)와 링크 키를 설정하기 위해 송수신한 메시지가 조합 키 메시지인 경우에는 조합된 결과에 의존하여 링크 키를 생성하고, 링크 관리자(106)는 조합 키 메시지를 송출하였으나 링크 관리자(116)가 단일 키 메시지를 송출한 경우에는 링크 관리자(116)의 키정보에 의존하여 링크 키를 생성하고, 링크 관리자(106)와 링크 관리자(116)간에 송수신한 메시지가 단일 키 메시지인 경우에는 링크 관리자(106)의 키정보에 의존하여 링크 키를 생성한다. 이와 같이 링크 키가 생성되면, 인증절차를 완료하면서 링크를 설정한 뒤, 단계 210으로 진행되어 링크설정작업을 종료한다.

<28> 그러나, 분석결과, 수신된 메시지가 인증요구 메시지이면, 링크 관리자(106)는 단계 222로 진행되어 대응되는 인증응답 메시지를 종단부(108)를 경유하여 인증요구 수신측(110)으로 송출한다.

<29> 이에 따라 인증요구 수신측(110)은 단계 320에서 인증응답 메시지를 수신하고, 단계 322에서 수신된 인증응답 메시지가 유효한 지를 판단한다. 판단방식은 단계 206에서와 동일한 방식으로 이루어진다. 판단결과, 수신된 인증응답 메시지가 유효하지 않은 경우에는 단계 324로 진행되어 인증 실패처리를 하고, 단계 314로 진행되어 링크설정작업을 종료한다. 인증 실패처리는 단계 208에서와 동일하게 수행된다.

<30> 그러나, 단계 322에서 판단한 결과, 수신된 인증응답 메시지가 유효한 경우에는 단계 326으로 진행되어 미 도식된 관리 테이블에 저장되어 있는 링크 키 생성을 위한 메시지를 이

용하여 링크 키 생성을 위한 메시지를 종단부(118)를 통해 인증요구 개시측(100)으로 송출한다. 그리고, 단계 328로 진행되어 상호인증 절차를 완료하고, 해당되는 링크를 설정한 후, 링크설정작업을 종료한다.

<31> 인증요구 개시측 링크 관리자(106)는 단계 222에서 인증응답 메시지를 송출한 후, 단계 224에서 링크 키 생성을 위한 메시지가 수신되면, 단계 226으로 진행되어 해당되는 링크 키를 생성하고, 상호인증 절차를 완료한 후, 링크를 설정한 다음 단계 210으로 진행되어 링크설정작업을 종료한다.

<32> 한편, 단계 212에서 링크 관리자(106)가 체크한 결과, 현재의 링크설정단계가 초기접속단계가 아니면, 단계 228로 진행되어 연결(connection) 설정 완료 메시지(LMP_setup_complete)를 인증요구 수신측(110)으로 송출하고, 송출된 연결 설정 완료 메시지를 미 도시된 관리 테이블에 저장한다.

<33> 이에 따라 인증요구 수신측(110)의 링크 관리자(116)는 단계 306에서 연결 설정 완료 메시지를 수신하고, 단계 308로 진행되어 상술한 바와 같이 자신의 인증조건을 체크하게 된다. 체크결과, 상호인증이 필요하지 않은 경우에는 단계 308를 통해 단계 310으로 진행되어 연결 설정 완료 메시지를 송출하고, 단계 312로 진행되어 상술한 바와 동일한 작업을 수행한다.

<34> 그러나, 단계 308의 체크결과, 상호인증이 필요한 경우에는 단계 316으로 진행되어 수신된 연결 설정 완료 메시지를 미 도시된 관리 테이블에 저장한 뒤, 단계 318로 진행되어 인증요구 메시지를 인증요구 개시측(100)으로 송출한다.

<35> 인증요구 개시측(100)의 링크 관리자(106)는 단계 228에서 연결 설정 완료 메시지

를 송출한 후, 단계 230에서 상대 장치인 인증요구 수신측(110)으로부터 메시지가 수신되면, 단계 232로 진행되어 수신된 메시지가 인증요구 메시지인지, 연결 설정 완료 메시지인지를 분석한다. 분석방식은 단계 218에서와 동일하게 이루어진다.

<36> 분석결과, 수신된 메시지가 연결 설정 완료 메시지이면, 단계 324로 진행되어 인증절차를 완료하고, 해당되는 링크를 설정한 후, 단계 210으로 진행되어 링크설정단계를 종료한다. 그러나, 분석결과, 수신된 메시지가 인증요구 메시지이면, 단계 236으로 진행되어 그에 대한 인증응답 메시지를 인증요구 수신측(110)으로 송출한다.

<37> 인증요구 수신측(110)의 링크 관리자(116)는 인증응답 메시지가 수신되면, 단계 320에서 단계 322로 진행되어 상술한 바와 같이 수신된 인증응답 메시지가 유효한지를 판단한다. 판단한 결과, 수신된 인증응답 메시지가 유효하지 않으면, 단계 324로 진행되어 상술한 바와 같이 운영된다. 그러나, 수신된 인증응답 메시지가 유효하면, 단계 326으로 진행되어 미 도시된 관리 테이블에 저장되어 있는 연결 설정완료 메시지를 이용하여 연결 설정 완료 메시지를 인증요구 개시측(100)으로 송출한 뒤, 단계 328로 진행되어 상술한 바와 같이 운영된다.

<38> 인증요구 개시측(100)의 링크 관리자(106)는 단계 236에서 인증응답 메시지를 송출한 후, 단계 238에서 연결 설정 완료 메시지가 수신되면, 단계 340으로 진행되어 상호 인증 절차를 완료하고, 링크를 설정한 후, 단계 210으로 진행되어 링크설정작업을 종료한다.

<39> 상술한 링크 관리자간의 인증방법은 인증요구 개시측(100) 및 인증요구 수신측(110)이 해당되는 호스트(미 도시됨)와 통합된 구조로 구현된 경우에도 적용될 수 있다.

【발명의 효과】

<40> 상술한 바와 같이 본 발명은 블루투스 통신환경에서 운영되는 장치간에 링크를 설정할 때, 상대 장치의 인증조건을 고려하여 수행하는 링크 관리자간의 인증방법을 제공함으로써, 블루투스 통신환경에서 운영되는 장치간에 정확한 링크설정 결과를 얻을 수 있는 효과가 있다.

【특허청구범위】**【청구항 1】**

블루투스 통신환경에서 운영되는 장치에 구비되어 있는 링크 관리자간에 링크를 설정하는 방법에 있어서,

인증요구 개시측 링크 관리자로부터 인증요구 수신측 링크 관리자로 인증요구 메시지를 송출하는 제 1 단계;

상기 인증요구 메시지에 대한 인증 응답 메시지가 수신되면, 상기 인증요구 개시측 링크 관리자는 현재의 링크설정단계에 따른 소정의 메시지를 상기 인증요구 수신측 링크 관리자로 송출하면서 저장하는 제 2 단계;

상기 소정의 메시지가 수신되면, 상기 인증요구 수신측 링크 관리자는 자신의 인증조건을 체크하는 제 3 단계;

상기 인증조건을 체크한 결과, 상호인증이 필요하지 않은 경우에는 상기 소정의 메시지에 대한 응답 메시지를 상기 인증요구 개시측 링크 관리자로 송출하는 제 4 단계;

상기 인증조건을 체크한 결과, 상호인증이 필요한 경우에는 상기 소정의 메시지를 저장하고, 상기 인증요구 개시측 링크 관리자로 인증요구 메시지를 송출하는 제 5 단계;

상기 인증요구 개시측 링크 관리자로부터 상기 인증요구 메시지에 대한 응답 메시지가 수신되면, 저장된 상기 소정의 메시지에 대한 응답 메시지를 상기 인증요구 개시측 링크 관리자로 송출하는 제 6 단계;

상기 인증요구 수신측 링크 관리자로부터 상기 소정의 메시지에 대한 응답 메시지가 수신되면, 인증절차를 완료하는 제 7 단계를 포함하는 링크 관리자간의 인증방법.

【청구항 2】

제 1 항에 있어서, 상기 제 2 단계 및 제 6 단계는,

상기 인증 응답 메시지가 수신되면, 자신이 보유하고 있는 키정보와 인증요구 메시지 송출시 이용한 랜덤 정보를 이용하여 수신된 인증 응답 메시지가 유효한 지를 판단하는 단계 ;

상기 판단단계 수행결과, 수신된 인증 응답 메시지가 유효하지 않으면, 인증 실패처리를 하고 링크설정작업을 종료하는 단계를 각각 더 포함하는 것을 특징으로 하는 링크 관리자간의 인증방법.

【청구항 3】

제 1 항에 있어서, 상기 제 2 단계에서의 상기 소정의 메시지는 상기 현재의 링크 설정 단계가 초기접속단계이면, 링크 키 생성을 위한 메시지가 되고, 상기 현재의 링크 설정단계가 초기접속단계가 아니면, 연결 설정 완료 메시지가 되는 것을 특징으로 하는 링크 관리자간의 인증방법.

【청구항 4】

제 3 항에 있어서, 상기 소정의 메시지는 상기 연결 설정 완료 메시지인 경우에 생성하고자 하는 링크 키가 상기 인증요구 개시측의 링크 관리자가 보유하고 있는 키정보와 상기 인증요구 수신측 링크 관리자에서 보유하고 있는 키정보의 조합결과에 의존할 것인지 상기 인증요구 개시측의 링크 관리자가 보유하고 있는 키정보에만 의존할 것인지에 따라 결정된 메시지가 송출되고, 상기 소정 메시지에 대한 응답 메시지는 상기 링크 키를 상기 조합결과에 의존하여 생성할 것인지, 상기 인증요구 수신측 링크 관리자가 보유하고 있는 키정보 또는 상

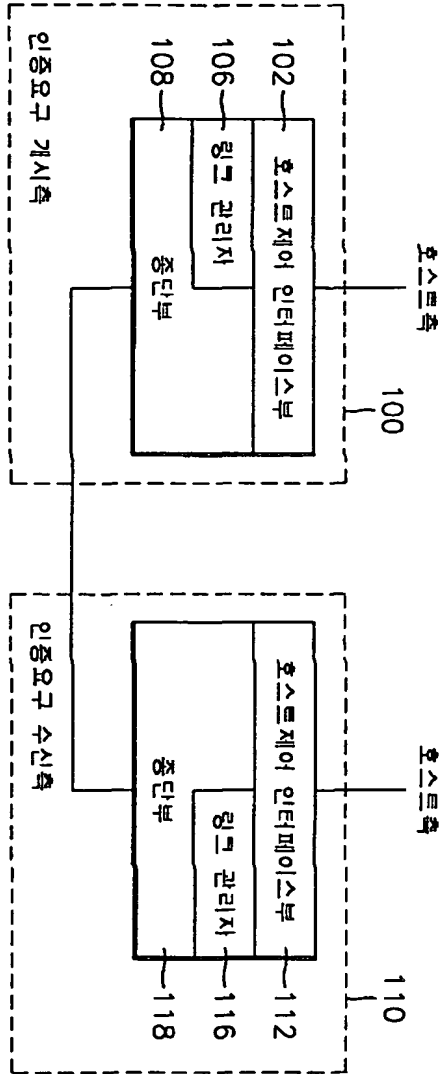
기 인증요구 개시측 링크 관리자가 보유하고 있는 키정보에 의존하여 생성할 것인지에 따라 결정된 메시지를 송출하는 것을 특징으로 하는 링크 관리자간의 인증방법.

【청구항 5】

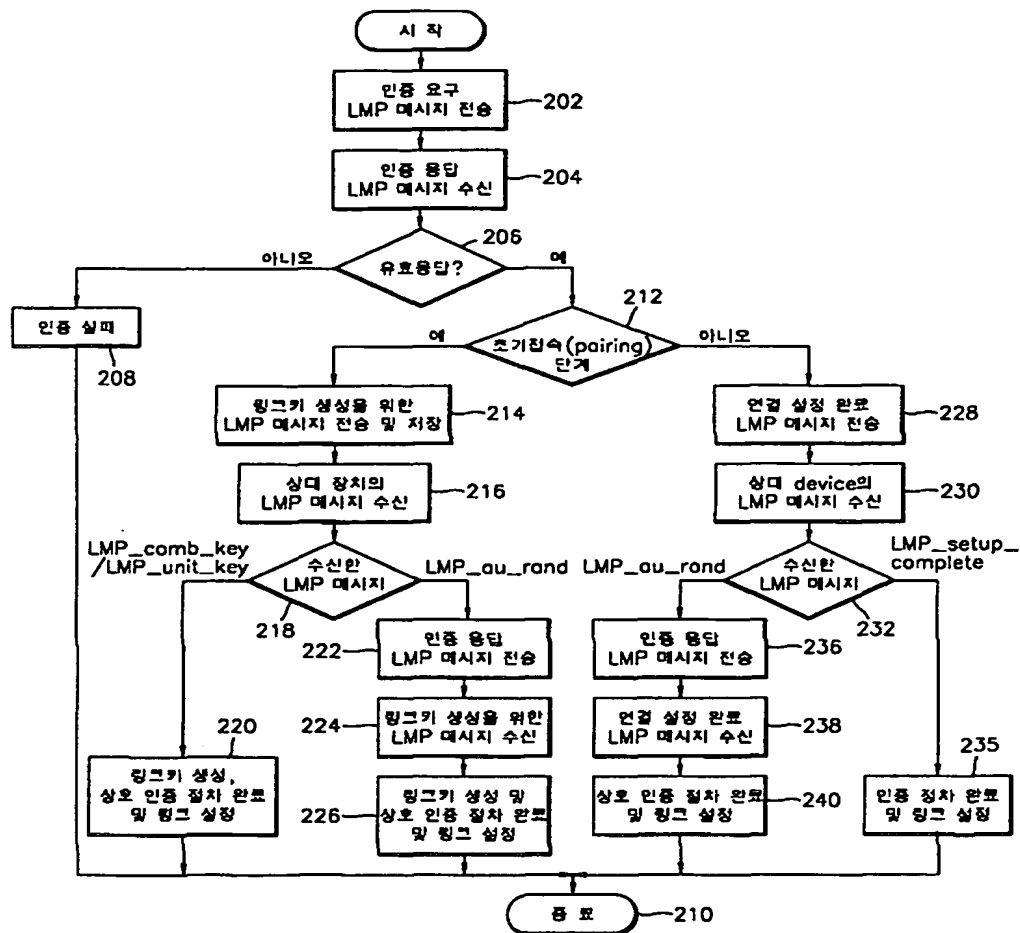
제 1 항에 있어서, 상기 제 3 단계는 보유하고 있는 인증 인에이블정보를 상기 인증조건으로서 체크하는 것을 특징으로 하는 링크 관리자간의 인증방법.

【도면】

【내 1】



【도 2】



【도 3】

